Information Systems Security Policy Handbook

Replaces: Information Systems Security Policy Adopted October 2003
Approved By: Bill Schrier, CTO

TABLE OF CONTENTS

Information Systems Security Policy Handbook

Replaces: Information Systems Security Policy Adopted October 2003
Approved By: Bill Schrier, CTO

INTRODUCTION

The purpose of this handbook is to consolidate and define the policies that help ensure the security and availability of City of Seattle information technology systems and networks. It also helps ensure the confidentiality, integrity and availability of electronic information captured, stored, maintained, and used by the City of Seattle. It provides direction for compliance to federal and state regulations, specifies appropriate practices, and defines custodial responsibilities for records associated with City operations. This policy should be used as a foundation document for all standards, procedures, and guidelines that are developed and implemented by the City related to information systems security.

All Users of City computing services, resources and data are required to support this effort by complying with all established policies, guidelines, and procedures. This includes compliance with all related federal and state statutes and regulations as required.

Prominent among these requirements is the City's commitment to ensure that its treatment, custodial practices, and uses of "Personally Identifiable Information" (See SECTION 4. DEFINITIONS) are in full compliance with all related statutes and regulations, and the City's core values of maximizing trust, integrity and respect for privacy.

It also is critically important to secure systems and networks from unauthorized access, to prevent their use for illegal activities, and to prevent their unwarranted destruction.

AUTHORITIES AND COMPLIANCE

The City of Seattle is a public entity. It has custodial responsibilities for a significant and diverse amount of sensitive information. It holds business contracts with a broad range of public and private organizations. It is the recipient of federal and private grants. It owns, maintains and operates significant critical infrastructures and services. All of these facts place significant burdens on the City regarding the management and use of its extensive information systems resources. Not least among these burdens are compliance requirements with many State and Federal laws, regulations, and promulgated rules. Beyond strict compliance requirements, the City must also understand and consider several additional government and industry standards and best practices that contribute to the objective of "due care."

Some State and Federal statues and regulations that may directly or indirectly affect City information systems security policy and operational guidelines can be found in "Appendix A" attached to this policy handbook.

The information contained in Appendix A is for the reader's convenience only. It should be understood that the City makes no representation as to the completeness, accuracy, or currency of the materials.

In addition to the City's compliance requirements, this policy also reflects the City's strong commitment to ethics and values that meet citizens' high expectations for responsible operations.

Successful compliance and protection of information systems assets requires all computing system owners, operators, and users of City-owned computing and network services, to read, understand, and support this **"Information Systems Security Policy Handbook"** and all related operational policies and procedures.

APPLICABILITY

This Policy is applicable to all users (employees, contractors, and others) of City computing systems, networks, digital information, and any other electronic processing or communications related resources or services provided through the City.

HANDBOOK ORGANIZATION

This handbook is organized in the following manner:

Back to Table of Contents

SECTION 1 – POLICY

POL01 Responsibilities of the Office of Information Security (OIS)

The Office of Information Security's (OIS) primary role is to provide strategic oversight, direction and coordination of a City-wide information systems security program and compliance efforts. See PRO01 Office of Information Security Tasks for details.

Back to Table of Contents

POL02 Responsibilities of the Information Technology Security Board

The Information Technology Security Board (ITSB) is an ad hoc committee whose role is to provide oversight and direction regarding information systems security and privacy assurance. The membership of the ITSB is composed of information technology management and staff representing the various departments and key administrative areas of the City's operations. See PRO02 Information Technology Security Board Tasks for details.

Back to Table of Contents

POL03 Responsibilities of System Owners

System Owners (See SECTION 4. DEFINITIONS) play a critical role in the protection of City Information Systems and data. They must manage and protect the data systems they are responsible for. To do so they must ensure compliance with information security policy and all statutory and regulatory requirements; ensure confidentiality, integrity and availability of their systems; and support user compliance with all City and departmental security policies. See PRO03 System Owner Tasks for details.

Back to Table of Contents

POL04 Responsibilities of Information Technology Managers

Information Technology Managers (See SECTION 4. DEFINITIONS) play a critical role in the protection of City Information Systems and data. IT Managers hold accountability for operational decisions about the use and management of a computing system and support the responsibilities of System Owners as noted in

POL03 Responsibilities of System Owners. See PRO04 Information Technology Managers Tasks for details.

Back to Table of Contents

POL05 Responsibilities of System Administrators

System Administrators (See SECTION 4. DEFINITIONS) hold a unique and powerful position in their relatively unfettered access to and maintenance of City systems and data. They must understand and follow City and departmental information security policy and observe the highest ethical and professional standards at all times (see "System Administrator Code of Ethics" in Appendix B). See PRO05 System Administrator Tasks for details.

Back to Table of Contents

POL06 Responsibilities of Data Custodians

The role of the Data Custodians (See SECTION 4: DEFINITIONS) is to provide direct authority and control over the management and use of specific information. These individuals might be Supervisors, Managers, Department Heads, or designated professional staff. They might serve dual roles as a System Owner/Operator as well as a Data Custodian. They typically would not be the technicians (system administrators) that support the related computer systems or applications. They are responsible for following all security policy and guidelines to protect and ensure the confidentiality of any sensitive data they control. See PRO06 Data Custodian Tasks for details.

Back to Table of Contents

POL07 Responsibilities of Users

All Users (See SECTION 4. DEFINITIONS) have a critical role in the effort to protect and maintain City information systems and data. Users of City computing resources and data must comply with all federal and state statutes, City ordinances, and City and departmental policies. All Users are required to attend and complete at least one information security awareness class or briefing and provide proof of attendance to their personnel staff to be included in their personnel record. See PRO07 User Tasks for details.

Back to Table of Contents

POL08 Monitoring of User Accounts, Files, and Access

1. **The City reserves the right to monitor its information systems and user activity. There is no guarantee of privacy of email, Internet access, system logs, and electronic files related to individual City computer and network accounts.**

2. **Inappropriate, unauthorized use or abuses of computing and network resources are subject to monitoring and investigation by authorized City staff.**

3. **Individuals and associated accounts under investigation are subject to having their activities on City systems monitored and recorded.**

4. **In the course of monitoring individuals who are improperly using these systems, or in the course of correcting system problems caused by the unauthorized use, the activities and files of authorized users may also be disclosed.**

5. **The City may specifically and without notice monitor the activity and accounts of individual users including files, session logs, content of communication and Internet access for adherence to the Acceptable Use Policy - POL17 (See GUI08 Monitoring of User Activity).**

6. **The City reserves the right to filter Internet access to preclude dangerous or harmful website connections.**

7. **Evidence of criminal activity will be turned over to appropriate City and law enforcement officials.**

8. **Some files and records may be subject to public disclosure laws and it is the responsibility of management and users to understand and comply with those laws (See Records Retention information in Appendix B - Related Documents).**

Back to Table of Contents

POL09 Administrative Access to City Information Systems

This policy applies to System Owners, Information Technology Managers (see Section 4 - Definitions), or other City management that grant administrative access to City IT Systems to any person or entity. Administrative access must only be granted based on an established and documented business need. The Procedure outlined in PRO09 Procedure for Granting Administrative Access to City Information Systems must be followed.

Back to Table of Contents

POL10 Electronic Data and Records Management

1. **All City System Owner/Operators, Data Custodians, and Users are obligated to understand the nature and proper classification of the data they generate, use, or store.**

2. **All City System Owner/Operators, Data Custodians, and Users(see Section 4 - Definitions), are required to properly manage and protect the confidentiality of private or sensitive electronic data they may be using, transmitting, and storing. For classification guidelines and best practices see GUI10A Classification of Data.**

3. **All City System Owner/Operators, Data Custodians, and Users are required to understand and comply with all records retention laws for any electronic data they may be using, transmitting, and storing.**

NOTE: Be aware that the City Records Management Program (CRMP) maintains specific records management information and offers consultation to users and management on their retention obligations under State law.

Back to Table of Contents

POL11 Electronic Data Breach Disclosure

A "reportable security breach" is defined by Washington State and Federal law. The City of Seattle will comply with all applicable laws. See PRO11 Electronic Breach Disclosure Procedure for details of the procedure to follow if a breach is suspected.

Back to Table of Contents

POL12 Access Controls

Access control measures required for establishing Users' access to any City computing resources shall be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved. See GUI12B Access Control Measures for direction on how to assess and define the appropriate security measures for computing systems.

1. **It is the responsibility of all System Owner/Operators and Data Custodians to ensure that their systems are properly protected.**

2. **Systems are required to have a technical access control mechanism (see GUI 12B).**

3. **All systems are required to have the capability to log basic information about User access activity, system events and errors, and access violation reports.**

4. **All system access accounts for Users must be based on a unique identifier.**

5. **No shared accounts are allowed.**

6. **All Users' system access will be based on the "principle of least privilege" and the "principle of separation of duties" (See Section 4 - Definitions).**

7. **Computer applications that are developed for the system must be developed and integrated to maintain individual user accountability and audit capability.**

8. **Documented procedures must be in place for issuing, altering, and revoking access privileges on shared systems.**

9. **Any vendor that requires access to City equipment must obtain written permission from departmental IT Management (See PRO12 Setting up Vendor Access to the Network. See also related policy POL21 Remote and Ad Hoc Connectivity).**

10. **Automatic Workstation Screen Locking - All City workstations must automatically go into a password-protected screen-lock mode after twenty (20) minutes of inactivity.**

Back to Table of Contents

POL13 Systems and Network Security

All systems and network security measures must be based on the functional nature and degree of criticality of the computer systems, network resources, and data involved. See GUI12A Assessing What Security Measures to Implement for direction on how to define the appropriate security measures for computing systems.

1. **It is the responsibility of all System Owner/Operators (see Section 4 - Definitions) to ensure that they have implemented all necessary security measures.**

2. **Operating systems must be maintained with the timely application of all related vender-issued patches (see GUI13A Operating System Maintenance).**

3. **Where appropriate, systems must have anti-virus software and maintain procedures for regular signature updates (see GUI13C Antivirus Measures).**

4. **Procedures must be maintained for regular backup of all data and system files necessary for recovery purposes (see GUI13D Backup, Recovery and Data Retention).**

5. **All systems are required to have the capability to log basic information about User access activity, system changes, and events, and all event logs must be converted to syslog format to enable central collection and monitoring. Web applications must create and send syslogs to a centralized syslog server. Infrastructure devices must log to a Security Incident Management (SIM) device. Firewalls and Intrusion Detection System sensors must route alerts to a SIM device (see GUI13B Logging).**

6. **All systems must maintain a functioning and accurate system clock**

7. **Encryption capabilities and secure protocols must be available for systems that contain, send or receive restricted or confidential data (see GUI13F Encryption).**

8. **Any transport of confidential or restricted data must use a secure transport protocol and/or be encrypted using the Encryption standards referred to in GUI13F Encryption.**

9. **All computing systems and servers hosted on City networks must support proactive vulnerability probing and reporting (see GUI13E Firewalls and Intrusion Detection Security).**

10. **System Owner/Operators (see Section 4 - Definitions) must ensure that no function, application, or other computing process is executed on their system(s) that uses an unreasonably large amount of bandwidth on City networks**

11. **USB connected, serial, or other portable devices are not allowed to be connected to City systems unless and until an exception request stating a legitimate business reason is received and accepted by the Office of Information Security.**

12. **Unauthorized, non-City owned and managed network devices (i.e firewalls, switches, routers) are not allowed to be connected to City systems at any time.**

13. **Any device containing a modem or other external connection and containing an operating system is not allowed to be connected to City systems without a written exception approval from the Office of Information Security (OIS). Exception requests will not be granted unless these deployments adhere to strict configuration guidelines as outlined in GUI13J Multifunction Device Configuration Guidelines.**

14. **System Owner/Operators (see Section 4 - Definitions) must display security-warning banners prior to allowing the access logon process to be initiated by Users (For an example see GUI13I Use of Security Warning Banner).**

15. **All servers deemed critical to City business functions and/or containing confidential or restricted data must have Host Intrusion Detection/Intrusion Prevention systems installed with alerts routed to a SIM device as noted in #8 above.**

Back to Table of Contents

POL14 Physical Security

As with logical security measures at the City, physical security measures required for protecting City computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved.

1. **Physical access control measures must be implemented sufficient to prevent City assets from unnecessary and unauthorized access, use, misuse, vandalism, or theft (See GUI14 Physical Security Guidelines for detailed guidance).**

2. **Certified smoke and fire alarm and fire suppression systems must be in place for larger data centers, server rooms and telecommunication closets and vaults.**

3. **Environmental control measures (power supply, heating, ventilation, air conditioning, plumbing, physical location) must be in place and monitored, tested and maintained regularly.**

4. **Inventory Control measures must be implemented, such as asset tags or other identification markings for tracking and accounting of City assets.**

5. **The City must have secured off-site data/media storage and procedures.**

6. **Specific procedures and security education for all Users of City laptops, wireless services, and other mobile computing devices must be instituted.**

7. **All specific tools, systems, or procedures implemented to meet physical security requirements will be selected on the basis of its ability to meet City specifications and performance requirements and be purchased in compliance to the City's procurement policies and procedures.**

Back to Table of Contents

POL15 Personnel Security Measures

1. **When hiring employees for key technical positions, comprehensive pre-employment screening must take place.**

2. **All pre-employment inquiries must be conducted in full compliance with all official City and specific departmental policies and in full compliance with all related state and federal laws.**

3. **New employees must be informed about their responsibilities and the policies that apply.**

4. **All employees are required to complete yearly training on the basic tenets of this information security policy.**

5. **All physical and logical access to computing and network facilities and resources must be assigned with the principles of least privilege and separation of duties applied (See Definitions - Section 4).**

6. **When terminating employees all City departments must establish processes to quickly close and remove all system and network privileges (See GUI15 Suggested Components of User Termination Process for examples).**

7. **Related procedures regarding employee suspension, leave of absence, long term illness or disability must also be established and maintained.**

Back to Table of Contents

POL16 Policy Enforcement

Violators of this policy may be denied access to City computing and network resources and may be subject to other civil suits and disciplinary action within and outside the City. Violations of this policy will be handled in accordance with the City's established disciplinary procedures.

1. **If incidental violations of this policy are discovered, the City will take appropriate actions to resolve the issue and violators may be subject to disciplinary measures.**

2. **If violations of this policy initiated by careless or deliberate acts are discovered, the City will take appropriate actions to resolve the issue which may include disciplinary measures up to and including separation of employment.**

3. **If violations of this policy are discovered that are illegal activities, the City will notify appropriate authorities.**

4. **The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of violations of this policy.**

Back to Table of Contents

POL17 Acceptable Use of City Digital Equipment, Internet Access, Electronic Communications and Other Applications

1. **City owned digital equipment, access to the Internet, and City provided applications may not be used for purposes that are prohibited by City of Seattle policy, ethics rules, or City, State or Federal law (See GUI17A Prohibited Uses of City-owned Digital Equipment for details).**

2. **Digital equipment and all applications must be authorized and installed by appropriate personnel in each City department (See GUI17B Installation of Hardware/Software for details).**

3. **Streaming video, audio or music files, image storage and other bandwidth or storage intensive features must be used judiciously and with strict business justification (See GUI17C Use of Bandwidth Intensive Application/Features for details).**

4. **Any network usage that might put an undo strain on City resources must be approved in writing by the CTO before implementation.**

5. **Resources of any kind for which there is a fee, whether accessed via the Internet, email or other applications, must not be accessed or downloaded without prior approval from a supervisor.**

6. **Use of any of these resources must be consistent with applicable Electronic Records Retention Laws and Policies (See Appendix B - Related Documents).**

7. **Nothing in these policies confers a right to privacy in digital data upon any person and the City reserves the right to monitor any and all activities on its equipment and to filter content (see POL08 Monitoring of User Accounts, Files, and Access).**

8. **The use of proxy servers (See Section 4 - Definitions) to avoid detection of non-business related Internet activities is prohibited.**

9. **Viewing or printing of written or graphic materials that denigrate or show hostility or aversion to an individual or group is prohibited. (see Personnel Rule 1.1 "Workplace Harassment" Appendix B - Related Documents).**

10. **Minimal use of City owned digital equipment, access to the Internet, and City provided applications including email for personal purposes is allowed (For details see GUI17D Guidance on De-Minimus Use of City Digital Equipment).**

Back to Table of Contents

POL18 Rules Specific to Electronic Communication Usage

1. **Electronic communication (e-mail, IM, IRC, SMS) is a temporary medium and, therefore, inappropriate for substantive policy messages.**

2. **Electronic communications that contain substantive policy messages must be archived either electronically or by printing out and saving a hard copy.**

3. **Individual users may use methods for screening their e-mail (See GUI18A Individual Screening of E-Mail).**

4. **Electronic communications sent to members of the public must be consistent with the City's Online Privacy and Security Policy (See GUI18B Guidance for Sending Public Electronic Communications).**

5. **Any outgoing messages which do not reflect the official position of the City of Seattle or the user's department must include the following disclaimer: "The opinions expressed here are my own and do not necessarily represent those of the City of Seattle."**

6. **All general distribution messages must contain the name of the approving authority (departmental e-mail administrator or designee) and the date of approval (See GUI18C Guidelines for General Distribution Message Within or Between City Departments for details).**

7. **All requests for citywide broadcasting must be sent to the GroupWise Administrator e-mail account (See PRO18 Procedure for Sending Citywide Broadcast for the specific procedures to follow).**

8. **Departments must implement department level guidance, where appropriate, regarding the departmental use of electronic communications.**

9. **Each department shall identify a Departmental e-mail administrator who will enforce and monitor this policy.**

10. **Only City standard applications may be used for any type of electronic communications, including e-mail and Instant Messaging (IM) unless a business need has been documented and an exception granted by the OIS (See Standards documentation in Appendix B - Related Documents. For exception see PRO24 Obtaining Exceptions to Information Security Policies).**

11. **Standard configurations must be conformed to for all electronic communications systems (See E-Mail Standards and IM Standards).**

12. **Instant Message systems specifically are not allowed to accept inbound attachments or links and must only use the user's seattle.gov email address as an identifier.**

13. **All Users are required to understand and comply with all records retention laws for any electronic communications they transmit, store or disseminate.**

NOTE: Be aware that the City Records Management Program (CRMP) maintains specific records management information and offers consultation to users and management on their retention obligations under State law.

Back to Table of Contents

POL19 Patch Management

1. **All system and application software must have critical patches applied within the time frame designated by the notification from the OIS.**

2. **Departments must institute practices that require any locally or remotely attached devices have critical patches applied to system and application software.**

3. **Image files used to configure computing devices must be maintained at current patching levels and should be considered "untrusted images" (see Section 4 - Definitions) until scanned for compliance.**

4. **Departments must be able to provide records of their compliance with this policy within 24 hours of a request by the OIS.**

5. **If system or application software cannot be patched; departments must employ and document risk mitigating measures in order to minimize the probability of system compromise until such time as the software can be patched.**

6. **Decisions as to criticality will rest with the OIS.**

7. **Notice of Critical Patches will be disseminated by the OIS via email to identified contact persons for each department.**

8. **A contract for any new City system designed and/or deployed in collaboration with, or exclusively by, outside vendors shall include specific language clearly identifying the party to be responsible for patching and maintenance of that system and its attendant applications.**

9. **Vendor contracts will identify specific remedies for any damages caused by failure to maintain the system or its attendant applications, and will also identify the party responsible for incident response and repairs.**

10. **Exceptions to this policy may be granted as necessary (see PRO19A Obtaining Exceptions to Patch Management Requirements).**

Back to Table of Contents

POL20 Virus/Malware Protection

1. **Departments will purchase and install anti-virus software for all LAN, application and database servers and workstations.**

2. **Antivirus software must be updated on a regular basis. Servers and workstations must be scanned periodically, either manually or via an automated program.**

3. **Servers that store, process or transmit restricted or confidential data (See GUI10A Classification of Data for data classification descriptions) in any form must be protected by a host-based intrusion detection system (HIDS) (See Section 4 - Definitions).**

4. **Departments will report all virus outbreaks that have extended beyond a single PC to their departmental service desk and to the Office of Information Security (OIS).**

5. **In the event of a serious virus outbreak, or threat to the City's network caused by malware, a computer or department may be disconnected from the network (See PRO 20A Disabling, Disconnecting an Infected Workstation or System for details of this process).**

6. **A serious virus outbreak or other threat to the City's network will result in the initiation of the Cyber Incident Response Plan (See PRO20B Initiation of the Cyber Incident Response Plan for details of the initiation process - Also see Addendum B - Related Documents for a link to the Cyber Incident Response Plan).**

Back to Table of Contents

POL21 Remote and Ad Hoc Connectivity

1. **All remote and ad hoc connections (Ad hoc devices are defined in Section 4 - Definitions) must be requested and approved in writing by departmental appointing authorities or their assigns; and by departmental IT management.**

2. **Departments granting remote access will ensure that authorized users and contracted vendors sign an Acceptable Use Agreement**
   - See PRO21 Remote-Ad Hoc Determination Process.
   - Also see PRO21-22B Acceptable Use Agreement for Remote/Ad Hoc/Wireless/VPN Access.

3. **Authorized users or contracted vendors must use only authorized methods for remote access to the Network and City services.**

4. **System owners and/or operators must terminate remote access mechanisms within one business day of notification that an authorized user or contracted vendors' privileges have been revoked.**

5. **It is the responsibility of the City to support authorized users of remote access and configure devices per PRO21A-1 VPN Connectivity Management Configuration Process.**

6. **The City is not responsible for the integrity, maintenance, and technical support of non-City owned computing and data storage devices, personal firewalls and software, etc. that may be used for connection to the Network.**

7. **General access to the Internet for recreational use through the Network is not permitted.**

8. **Authorized users who access City restricted or confidential data must be authenticated through access mechanisms as outlined in POL12 Access Controls.**
9. **Authorized and ad hoc users and contracted vendors are accountable for all activities while connected to the Network and will bear the consequences should the access privilege be misused.**

10. **Departments authorizing remote and ad hoc connections will establish appropriate connectivity management processes that will, at a minimum, audit and monitor for anti-virus signatures and**

required operating system patches.

11. **Departments authorizing remote and ad hoc connections will scan computing devices for the existence of malicious code and programs.**

12. **All authorized remote and ad hoc devices will have automatic updates enabled by default.**

13. **Data classified as restricted or confidential must be protected in accordance with City procedure (See GUI10A Classification of Data for classification guidance).**

14. **Ad hoc computing devices will not be allowed to connect to the Network unless for the purpose of scanning and patching the device in a secure holding queue on the Network.**

15. **Ad hoc users who request connection to the Network must not introduce viruses, vulnerabilities, or other types of malicious code.**

16. **Ad hoc users who are connected the Network must not be connected to any other network at the same time.**

17. **Any device used to connect remotely to the City's Network must contain City standard anti-virus software, a personal firewall and operating system that are patched at the most up-to-date levels.**

18. **Any remote desktop access via a VPN tunnel will only use the City standard application, currently Terminal Services. Any other remote desktop applications must be requested using the policy exception process (PRO24 Obtaining Exceptions to Information Security Policies).**

19. **Home LAN to City LAN VPN site-to-site tunnels are not allowed.**

20. **Non-City owned networks and computing devices, used to connect remotely to the Network, must not be reconfigured for the purpose of split-tunneling or dual homing at any time.**

21. **Departments granting access to contracted vendors must ensure that access is limited to only specific and documented computing devices.**

Back to Table of Contents

POL22 Wireless Access

1. **Wireless technology is inherently insecure (see Section 4 Definitions - for specific examples of wireless technology). No wireless deployments are allowed unless a written business case has been received and reviewed and an exception to this policy is approved by the OIS.**

2. **Departments deploying devices with enabled wireless capability will ensure that authorized users and contracted vendors sign an Acceptable Use Agreement (see PRO21-22B Acceptable Use Agreement for Remote/Ad Hoc/Wireless/VPN Access for a sample Acceptable Use Agreement).**

3. **Departments deploying devices with enabled wireless capability for general use will ensure that an Acceptable Use Agreement is signed by the administrators of those devices.**

4. **System owners and/or operators must terminate and remove wireless enabled computing devices within one business day of notification that an authorized user or contracted vendors' privileges have been revoked.**

5. **Authorized users who access City restricted or confidential data must be authenticated through access mechanisms as outlined in POL12 Access Controls in this handbook.**

6. **Authorized users and contracted vendors are accountable for all activities while connected via wireless enabled computing devices and will bear the consequences should the access privilege be misused.**

7. **Wireless devices must be deployed with a software or hardware host firewall application or device.**

8. **Data classified as restricted or confidential must be protected in accordance with City Procedures (see GUI10A Classification of Data for classification guidelines).**

9. **All City owned and managed wireless networks connected to the City backbone will be so identified with a welcome banner as referenced in GUI13I Use of Security Warning Banner.**

10. **Dual homing is not allowed, so wireless devices must be setup with separate profiles for wireless and wired connections.**

Back to Table of Contents

POL23 Web Application Deployment

Departments deploying Internet (Web) based applications must follow City standards to ensure the confidentiality, integrity, and availability of any data accessed, managed, or stored by those applications. (Please see Appendix B-Related Documents for a link to Web Application Deployment standards and procedures)

Back to Table of Contents

POL24 Policy Exceptions

Exceptions to any part of this policy (other than exceptions to patch management requirements as noted in POL19 and PRO19A) must be requested using PRO24. Exceptions must be completed and signed by departmental appointing authorities and include a complete and explicit business case. Decisions on the acceptance or rejection of exception requests lie with the Office of Information Security (OIS) or assigns. Rejected requests may be appealed to the CTO.

Back to Table of Contents

SECTION 2 – PROCEDURES/TASKS

PRO 01 Office of Information Security Tasks

1. **The OIS acts as Chairperson of the Information Technology Security Board (ITSB)**

   The OIS will schedule meetings as required for information security policy or standards deliberations. They will create the agenda; chair the meetings; and record minutes. Agenda and minutes will be retained and made available via the Technology Security InWeb site.

2. **The OIS will provide information as necessary to City department management about existing and emerging legal and compliance requirements**

   The OIS will keep up to date on changing compliance rules and regulations and industry best practices. They will make every effort to relay those changes to affected City departments and will be available to department management for consultation.

3. **The OIS will support security awareness and education program efforts**

   The OIS will create, promote and disseminate information security awareness curriculum. They will make this training available to all City employees and users of the City network.

4. **The OIS will provide direction and support for City-wide information systems security policies and procedures**

   The OIS will support the development, implementation, maintenance and enforcement of City-wide or departmental information systems security policies, procedures, and tasks. They will be available for consultation, editing, or leading development teams.

5. **The OIS will ensure that vendors, business partners and others are aware of City security policies**

   The OIS will make security policies and procedures available to vendors, business partners and others. They will ensure that City procurement, contracting and partnering processes not only emphasize adherence to security policies but where appropriate incorporate provisions which

punish failures to properly address and comply with the policies.

6. **The OIS will provide direction and oversight concerning risk management practices associated with information management, privacy issues and industry best practices**

   The OIS will establish risk management practices and work with the City's Auditors and Office of Risk Management.

7. **The OIS will support appropriate audit services and reporting**

   The OIS will work with City Auditors to detect violations; to evaluate the effectiveness of policies and of compliance activities; and to ensure the use of information security industry recognized best practices.

8. **The OIS will review all exceptions to this policy**

   The OIS or assigns will review any requests for exceptions to this policy to ensure their appropriateness and legality (See PRO 23 – Obtaining Exceptions to Information Security Policies).

9. **The OIS will advocate for information security budget and resource requests**

   The OIS will work with Department of IT directors to research, select and test hardware and software that helps to ensure the maintenance of effective information systems security programs. He/she will help define requirements and compare solutions to ensure the greatest possible value and efficacy.

Back to Table of Contents

PRO 02 Information Technology Board Tasks

The ITSB will:

1. **Oversee** the development, implementation and enforcement of City-wide *Information Systems Security Policy* and related recommended guidelines, operating procedures and technical standards

2. **Meet as needed** to deliberate and revise the City-wide *Information Systems Security Policy* and related recommended guidelines, operating procedures and technical standards

3. **Advise** the OIS on any department specific issues, threats, vulnerabilities or challenges that might adversely affect the City's overall information security

Back to Table of Contents

PRO 03 System Owner Tasks

System owners must:

1. **Ensure** the confidentiality of sensitive proprietary data especially personally identifiable information (See PRO 10A – Classification of Data).

2. **Grant access** to users based on the "Principle of Least Privilege" (See SECTION 4. DEFINITIONS) where required

3. **Grant access** to their systems based on the "Principle of Separation of Duties" (See SECTION 4. DEFINITIONS) where required

4. **Document and submit for review** to the ITSB any desired exceptions to City-wide policy (See PRO 23 – Obtaining Exceptions to Information Security Policies).

5. **Support** any incident response activities that involve their system(s)

6. **Advocate for** security resources as required in City budget processes and in grant proposals

Back to Table of Contents

PRO 04 Information Technology Managers Tasks

1. **Document and report** to the OIS and appropriate security services personnel all incidents of security breaches

2. **Work closely with** the ITSB, the OIS, Data Custodians, and System Owners to help ensure the successful protection of City computing resources and data

Back to Table of Contents

PRO 05 System Administrator Tasks

System Administrators will:

1. **Monitor and maintain** network and messaging user accounts and passwords
2. **Maintain** equipment inventories
3. **Administer and lead** equipment and software purchasing and licensing management
4. **Maintain and update** servers and desktop operating systems and applications
5. **Direct** user desktop support and training
6. **Understand and comply with** the System Administrator Code of Ethics (see Appendix B – Related Documents)

Back to Table of Contents

PRO 06 Data Custodian Tasks

Data custodians will:

1. **Provide** the requirements to the System Owners and Operators for all access control measures related to the data they are charged with protecting
2. **Support** access control to data by acting as a single control point for all access requests.
3. **Support** regular review and control procedures that ensure that all users and associated access privileges are current and appropriate
4. **Work in conjunction with** the System Owner/Operator and the OIS to ensure that “due care” is taken to properly protect sensitive data

Back to Table of Contents

PRO 07 User Tasks

Users of City computing resources and data will:

1. **Protect and never share** access accounts, privileges, and associated passwords

2. **Maintain** the confidentiality of sensitive information to which they are given access privileges

3. **Accept** accountability for all activities associated with the use of their network accounts and related access privileges

4. **Ensure** that use of City computers, email and other electronic communications (IM, etc), Internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined use limitations

5. **Report** all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, system administrator or the OIS)

Back to Table of Contents

PRO 09 Procedure for Granting Administrative Access to City Information Systems

Because administrators are given unfettered access to City systems it is imperative that any time administrative access is granted the following procedure is followed. Exceptions may be granted (see PRO 23 – Obtaining Exceptions to Information Security Policies) if the position in question has an historic and accepted business need for administrative access.

Action By	***Action***
Dept Mgmt or Assigns	**1. Learns of** a need to grant administrative access to an employee or contractor.
	2. Determines through consultation with staff precise needs regarding systems and data to be accessed.
	3. Accounts for principles of "least privilege" and "separation of duties" (See: DEFINITIONS – Section 4).
	4. Decides to grant administrative access.
	4a. Works with DoIT or departmental IT staff to establish appropriate accounts and passwords.
	4b. Ensures Administrative user has read and understood "System Administrator Code of Ethics" (See Appendix B).
IT Staff	**5. Creates** account and password and **communicates** them to administrative user and department management or assigns
Dept Mgmt or Assigns	**6. Logs and Monitors** via weekly audits or an approved automated monitoring system all activities of the administrators**.**
	7. Verifies and Records yearly refresher training of this policy and the System Administrator code of Ethics.
	8. Reports any violations of this policy immediately to departmental Human Resources, appointing authorities and the OIS.
	9. Requests investigations using the City's Digital Investigation Procedures (See Addendum B – Related Documents).

PRO11 Electronic Breach Disclosure Procedure

If a breach of the City's electronic information systems is suspected the following procedure will be followed:

Action By	***Action***
IT Staff, Service Desk Personnel, or Dept Mgmt	**1. Receives** notice of possible data breach and **Notifies** department management.
Dept Mgmt or assigns	**2. Determines** through consultation with users and/or IT staff that it is an actual or suspected breach.
	3. Contacts OIS and DoIT Network Services for consultation and verification of breach.
	4. Isolates the system from the network.
	4a. Takes no immediate remediation action to avoid destruction of evidence.
	4b. Collaborates with OIS to establish next steps..
Office of Information Security (OIS)	**5. Determines** nature of the breach and assigns a severity level (See PRO 20B – Initiation of Cyber Incident Response Plan)
	6. Collaborates with department management to decide next steps
	6a Preserves the current status of the system for future investigation and/or
	6b Initiates an immediate investigation with the help of departmental subject matter experts and/or
	6c Invokes the City Cyber Incident Response Plan (See PRO 20B – Initiation of Cyber Incident Response Plan)
	7. Complies with all applicable breach disclosure laws based on the findings of the investigation.

Back to Table of Contents

PRO12 Setting up Vendor Access to the Network

There are cases where an outside vendor has a legitimate business need to access City systems for maintenance, updates or troubleshooting of their supported applications. In these cases, the following procedures should be followed:

Action By	***Action***
Dept Mgmt or Assigns	**1. Receives** notice of vendor requirement to access City systems and/or networks.
	2. Determines, through consultation with IT staff, vendor needs regarding time and frequency of access.
	3. Contacts OIS and IIT and/or DoIT Network Services for consultation on risks to the City's systems.
	4. Decides to grant vendor access.
	4a. Collaborates with DoIT or departmental Network Services to establish appropriate accounts and passwords.
	4b. Completes Acceptable Use Agreement and **obtains signatures** from vendors and supervisors.
Network Services Staff	**5. Creates** account and password and **communicates** them to vendor
	6. Establishes communications with vendor representative to maintain passwords and access controls**.**
	7. Maintains passwords, access controls and vendor communications on an ongoing basis. **NOTE:** Must be cognizant of vendor contract and end dates.
Vendor	**9. Assigns** representative to work with Network Services Staff.
	10. Signs and complies with all contracts and agreements.

Back to Table of Contents

PRO 18 Procedure for Sending Citywide Broadcast

At times it is necessary to send an e-mail broadcast to all employees in the City. Discretion must be used to ensure that these messages are of importance and value to all City users. To that end, the following procedure has been developed and must be followed:

Action By	***Action***
User	**1. Contacts** department/division management and/or departmental PIO with request to broadcast a message citywide.
Dept/Div Mgmt and/or PIO,	**2. Determines** through consultation with staff the message should be broadcast citywide.
	3. Edits (in consultation with user) message for clarity and correct information.
	4. Forwards message to the GroupWise Administrator and the Mayor's Office for approval.
GroupWise Administrator	**5. Assesses** the message for style and configuration correctness. If it needs modifications then: **5a Returns** the message to Dept/Div Mgmt or PIO with request for modifications, or if not: **5b Forwards** the message to the Mayor's Office for final approval, and **5c Informs** the Dept/Div manager or PIO by copying them on the message to the Mayor's Office.
Mayor's Office PIO	**6. Analyzes** the message to ensure it meets the standard of importance and value to all employees. If it does: **6a Returns** the message to the GroupWise Administrator stating the Mayor's Office approval for citywide broadcast. If it does not meet the standard, then: **6b Returns** the message to Dept/Div Mgmt or PIO, explaining reason for rejection (Dept can appeal directly to Mayor's Office)
GroupWise Administrator	**7. Distributes** a citywide broadcast of the message if it was approved.

Back to Table of Contents

PRO 19A Obtaining Exceptions to Patch Management Requirements

It is understood that there is a difference between critical patches and service packs (see definitions). These differences might result in a need for exceptions, especially as regards service packs. Exceptions to the Patch Management policy (POL 19 in this handbook) will be handled as follows:

Action By	*Action*
Dept Mgmt or Assigns	**1. Receives** notice of patch requirement from OIS.
	2. Determines through consultation with staff possible issues with deploying the patch in the required timeframe.
	3. Directs staff to accomplish testing and report their findings.
Dept. IT Staff	**4. Tests** patches for issues with any applications or operating systems.
	5. Reports findings back to Dept Management in a timely manner.
Dept Mgmt or Assigns	**6. Analyzes** findings and consults with staff.
	7. Determines if there is a need to request exception.
	7a. If need is established **determines** timeline for re-evaluation and acceptance of the patch, and **establishes** justification and risk mitigation.
	8. Writes letter, email, or completes form requesting exception from OIS. **NOTE:** Request must contain justification, mitigation and timeline to be considered.
Office of Information Security (OIS)	**9. Reviews** request and makes determination within 5 working days of receipt of request.
	9a. If rejected **meets with** requesting management or designee to discuss options and make final decision.
	10. Maintains copy of request and determination.

Back to Table of Contents

PRO 20A Disabling, Disconnecting an Infected Workstation or System

	Task to be performed	Action required	Performed By
1.	Create Heat Ticket and document your actions	Open a Heat Ticket and assign it to DoIT Network Engineering. Document the information you have about the workstation on the Heat Ticket.	Network Services or Service Desk or Desk Top
2.	Verify workstation needs to be disabled	Scan the device with Nessus looking for something that matches a Nessus signature as being a problem. Perform in-depth Nessus scan.	Network Engineering
3.	Determine nature and size of the problem **Not Severe**	One workstation and **Not Severe** problem. Can wait 24 hours to disable. Criteria for **Not Severe**: - Device disappears off the network - No current exploit running in memory Document the decision on the Heat Ticket. Continue with step **5.** **Decision: Not Severe**	Network Engineering
	Severe	One workstation with **Severe** problems. **Cannot** wait 24 hours to disable. Criteria for **Severe**: - Risk of affecting or infecting others Document the decision on the Heat Ticket. Continue with step **5.** **Decision: Severe**	
	Critical	**Critical** issue. **Cannot** wait 24 hours to disable. Must meet both these criteria for issue to be **Critical**: - team of staff is required to solve the problem - outage affects the work of several city employees or disrupts citizen's access to city services and information Document the decision on the Heat Ticket. Continue with step **4.** **Decision: Critical**	
4.	**Critical** Issues only	Activate Emergency Action Procedure located here: Send co-worker to notify OIS and DoIT Data Network Manager or other Operations Manager if they are not available. Continue with next step.	Network Engineering

	Task to be performed	Action required	Performed By
5.	**All Issues:** Identify IP address, customer name (if available) and Device Name	Nessus report contains the MAC address and will sometimes contain the User ID Report will contain the Device Name such as DoIT 1234565. Find Port Address by looking at the appropriate router switch. Find the department who owns the port – look at the port description on switch. Try to find the jack number – it might be on the port description. Find the IP address if possible. Use IP Address to find workstation name: Look at WINS Services Look at EPO Server Look at WSUS Service	Network Engineering and NOC
6.	Update Heat Ticket	In Heat system: - document all information on ticket - open an assignment to the NOC	Network Engineering
7.	Notify NOC	Call NOC at extension 6-1995 (outside phone number is 206-386-1995). Tell the NOC that a Heat Ticket to disable an infected workstation has been created and assigned to NOC.	Network Engineering
8.	Notify Service Desk	Call DoIT Service Desk 6-1212 (outside phone number is 206-386-1212). Tell the Service Desk that a Heat Ticket to disable an infected workstation has been created so the Service Desk can answer customer questions that may come to them.	Network Engineering
9.	Update Heat Ticket	In Heat system: - document Network Engineering actions on Heat Ticket - close Network Engineering assignment	Network Engineering

	Task to be performed	Action required	Performed By
10.	Notify department and customer Provide response information to the customer.	1. If **Severe** or **Critical** (not waiting 24 hours): - Call IT Department Contact **Pursue until personal contact is made with the department contact.** Provide response information shown below page. 2. If **Not Severe**, (able to wait 24 hours) - Call and send email to IT Department contact It is not necessary to make personal contact. Provide response information shown below page. <u>Response Information</u> Information to provide to the IT Department Contact for both 1 and 2 above: - Someone from Desktop will contact the department contact to find, disconnect, and fix the PC. - Your jack will be disabled (now or 24 hours from now) and you will not be able to connect to the network.	NOC
11.	**Decision: Wait 24 hours or not?**	If waiting 24 hours (**not severe**) stop and continue tomorrow with the next step. If **not** waiting 24 hours **(severe or critical) –** skip the next step and continue with the procedure immediately.	NOC
12.	Re-contact customer	If 24 hours has gone by, re-contact the IT Department Contact to tell them the port will be disabled now.	NOC
13.	Disable port and notify Desktop	Configure switch to disable the port. Notify Desktop and let them know to disconnect the workstation from the network. In Heat system: - document actions on Heat Ticket - open assignment to Desktop	NOC
14.	Disconnect the Workstation and re-enable port	Disconnect the Workstation from the network. Notify the Office of Information Security (OIS) if this is a **severe** or **critical** problem to forensically analyze the workstation before it is re-imaged. Notify the NOC to configure the switch to enable the port. In Heat system: - document actions on Heat Ticket	Desktop

	Task to be performed	Action required	Performed By
15.	Re-enable the port	Configure switch to enable the port. In Heat system: - close NOC assignment - document actions on Heat Ticket	NOC
16.	Forensically analyze severe and critical problems	**Critical** or **severe** infections must be forensically analyzed before the workstation is re-imaged and placed back into production. Follow the Digital Investigation procedures: Notify Desktop when the work is completed.	Office of Information Security (OIS) **Error! Reference source not found.**
17.	Re-image/Repair the workstation and test with the customer and NOC	Repair or re-image the workstation. Reconnect the workstation to the network. Notify the NOC that the customer will be testing the workstation so that port traffic can be monitored. In Heat system: - document actions on Heat Ticket - open a new NOC assignment - close Desktop assignment	Desktop
18.	Monitor the port	Notify Network Engineering that the port needs to be re-scanned with Nessus. In Heat system: - document actions on Heat Ticket - open new assignment to Network Engineering	NOC
19.	Verify that the port is no longer showing a problem	Use Nessus to scan the device. If the device is still infected, begin this procedure again at step 1. If problem is resolved, notify the NOC and the Office of Information Security (OIS) that the problem is resolved. In the Heat system: - document actions on Heat Ticket - close Network Engineering assignment	Network Engineering
20.	Close Assignment	In Heat system: - close NOC assignment - close the Heat Ticket	NOC
21.	Procedure Complete		

Back to Table of Contents

PRO 20B Initiation of the Cyber Incident Response Plan

Any event that significantly threatens the confidentiality, integrity or availability of the City's network and computer systems may be serious enough to initiate the Cyber Incident Response Plan. The procedures to initiate that plan are as follows:

Action By	***Action***
Service Desk Personnel, NOC, Operations on-call, or other personnel	**1. Reports** possibly serious event to OIS.
Office of Information Security (OIS)	**2. Determines** that event most likely meets the criteria for an event of Severity Level 1 or 2 as defined in the Cyber Incident Response Plan (see Appendix B – Related Documents).
	3. Contacts the Cyber Incident Response Team triage group and arranges meeting.
	4. Leads and facilitates the meeting of the triage group.
Cyber Incident Response Triage	**5. Establishes** the parameters and scope of the incident.
	6. Analyzes findings and consults with staff.
	7. Determines if there is a need to escalate or revise the severity level and/or initiate a formal incident response.
	7a. If need is established **contacts** affected personnel and department management, and **initiates** the incident response plan.
	7b. If incident response is deemed unnecessary, **documents** the event, the participants and the conclusions.
	8. Assigns Incident Commander and turns over command.
	9. Briefs Incident Commander with all available documentation and information regarding the event.

Back to Table of Contents

PRO21 Remote-Ad Hoc Determination Process

In order to implement the correct remote access or ad hoc connection solution several considerations and options must be weighed. The following procedure will give City management direction toward the most efficient and operationally sound solution.

Action By	***Action***
Dept Manager or Assigns	**1. Receives** request from employee, contractor, or vendor for a remote or ad hoc connection to the City's network
	2. Determines specific needs and best solution. If user needs:
	2a. Access to email and calendar only – Blackberry or GroupWise Web – go to GWWeb standards or Black-Berry standards
	2b. Cell phone access plus email and calendar – Blackberry – go to Blackberry standards
	2c. Access to InWeb applications or network drive data – CoS VPN with Citrix Metaframe – go to PRO 21A VPN Access Process
	2d. Full access to internal City network resources – CoS Non-Standard VPN access – go to PRO 21A VPN Access Process **(NOTE: requires OIS review and approval)**
	2e. Travel Access to Internet only – no sensitive information stored on digital equipment and no VPN or other access to City networks – 802.11 wireless card – go to 802.11x wireless standards
	2f. Travel Access to City network – Sensitive or confidential information stored on digital equipment and/or VPN or other access to City networks – CDMA wireless card – go to CDMA standards
	2g. Vendor, contractor, etc – require temporary connection to City Network via network jacks on City premises – Temporary wired access – go to Wired Access standards
	3. Follows appropriate solution process
	4. Develops business case if requesting Non-Standard VPN access and **Delivers** to OIS [click here for business case form]

	5. Develops exception business case if asking for exception to solution defined above - and **Delivers** to OIS [follow PRO 24]
Office of Information Security (OIS)	**6. Reviews** business case and **Assesses** risk
	7. Recommends for or against allowing Non-Standard CoS VPN access or any exceptions requested – providing explanation of opinion to department management and **Delivers** to Dept Manager or assigns
Dept Manager or Assigns	**7. Accepts** OIS decision or appeals to CTO
Chief Technology Officer (CTO)	**8. Makes** final decision and ruling on exception – documenting explanation of decision and delivering copies to OIS and department management

Back to Table of Contents

PRO21A VPN Access Process

If VPN access is the solution that best meets a City user's business requirements as determined by PRO21 – Remote-Ad Hoc Determination Process, this procedure should be followed.

Action By	***Action***
Dept Manager or Assigns	**1. Receives** request from employee, contractor, or vendor for a remote or ad hoc connection
	2. Determines using the Remote Ad-Hoc Determination Process that the best solution would be VPN access
	3. Determines which VPN solution is most appropriate given the user's business need:
	3a. CoS VPN - Access to InWeb Applications or network drive data – VPN with Citrix Metaframe
	3b. Non-Standard CoS VPN - Full access to internal City network resources – Full VPN access (requires OIS review and approval – fill out business case form and deliver to OIS)
	3d. Access to **GW Web email** – no VPN needed
	4. Gets signatures on a new user acceptable use agreement
Dept Service Desk	**5. Receives and Processes** requests – routing them to IIT or Network personnel as appropriate and logs information in HEAT
Network Services (IIT)	**6. Configures** user in appropriate VPN accounts
	7. Grants appropriate access to City services, directories.
Dept Service Desk	**8. Delivers** VPN software, or **Configures** City VPN device as appropriate and logs information in HEAT
	9. Verifies with user that VPN access is working correctly, **resolves** any problems and logs information in HEAT.
	10. Closes HEAT ticket

PRO21A-1 VPN Connectivity Management Configuration Process

For a device to be enabled for VPN access, it must be configured according to the following connectivity management requirements.

Action By	***Action***
Dept Manager or Assigns	**1. Receives** request from employee, contractor, or vendor for a remote or ad hoc connection
	2. Determines using the Remote Ad-Hoc Determination Process that the best solution would be VPN access
	3. Follows PRO21A to establish a VPN account for the user
	4. Determines which device will be used for VPN access – if non-City owned device (**CoS VPN only**) go to process **step 5.** If City owned device (**required for CoS Non-Standard VPN access)**, skip to process **step 6**
Dept Manager or Assigns	**5. Determines** if user's intended hardware for connection is running a City approved anti-virus application (see VPN Access Standard - STA 21A)**.** If yes, proceed to **6** - if no, complete exception process and submit to OIS for approval.
	6. Submits service request to department service desk for CoS VPN Access. **Skip to Step 9**
	7. Obtains signed OIS approval after submitting business case as required in PRO21A
	8. Submits service request to department service desk to have a City device configured for CoS Non-Standard VPN access.
Dept Service Desk	**9. Receives and Processes** requests – routing them to AD Group as appropriate and logs information in HEAT
Department desktop support staff or service desk personnel	**10. Delivers** CoS VPN Installation instructions to user, or **Configures** City owned device for CoS Non-Standard VPN access
Dept Service Desk	**11. Verifies** with user that VPN access is working correctly, **resolves** any problems and logs information in HEAT.
	11. Closes HEAT ticket

PRO 21-22B Acceptable Use Agreement for Remote/Ad Hoc/Wireless/VPN Access

Follow this link to access the current acceptable use agreement for VPN and Remote Access. This agreement may be used as an example for specific departmental or other acceptable use agreements:

Link to VPN Acceptable Use Agreement

Back to Table of Contents

PRO 24 Obtaining Exceptions to Information Security Policies

It is understood that different departments have differing business needs. These differences might result in a need for exceptions to any of the policies recorded in the Policies section of this handbook. Exceptions will be handled as follows:

Action By	***Action***
Dept Mgmt or Assigns	**1. Receives** information security policy clarifications or revisions from OIS.
	2. Determines through consultation with staff possible issues or conflicts with business needs of the department/division.
	3. Directs staff to research issues and alternatives and report their findings.
Dept. IT Staff	**4. Researches** issues and alternatives.
	5. Reports findings and recommendations to Dept Management in a timely manner.
Dept Mgmt or Assigns	**6. Analyzes** findings and consults with staff.
	7. Determines if there is a need to request exception.
	7a. If need is established **establishes** justification and risk mitigation.
	8. Writes letter, email, or completes form requesting exception from OIS. **NOTE:** Request must contain justification and risk mitigation to be considered.
Office of Information Security (OIS)	**9. Reviews** request and makes determination within 5 working days of receipt of request.
	9a. If rejected **meets with** requesting management or designee to discuss options and make final decision.
	10. Maintains copy of request and determination.

Back to Table of Contents

SECTION 3 – GUIDELINES

GUI 08 Monitoring of User Activity

As noted in POL08, there is ***no expectation of privacy*** when using City owned electronic equipment. There are many reasons that activity on the network and on individually used digital equipment might need to be monitored and recorded.

Monitoring of activities may be done without notice to users when:

- Activity from an account prevents access to computing and network resources by others;
- General usage patterns indicate that an account is responsible for unacceptable activity;
- There is reasonable cause to believe that user has violated or is violating policy or the law:
- It appears necessary to do so to protect the City from liability;
- Account activity is causing network interruptions or degradation of service; or
- It is required by and consistent with law.

Departmental IT Management and Human Resources staff are responsible for deciding when and how to monitor user activity on City owned electronic equipment. If an investigation is warranted they must follow the procedures as outlined in the Digital Investigation Procedures document, a link to which can be found in Appendix B – Related Documents.

Back to Table of Contents

GUI 10A Classification of Data

While the City does not employ any official data classification system per se, the following defined categories of data can be useful for System Owner/Operators and Data Custodians to understand appropriate protection requirements.

- **PUBLIC:** Information that is either approved for general access or by its nature not necessary to protect and can be shared with anyone. This would include general public information, published reference documents (within copyright restrictions), open source materials, approved promotional information, and press releases.

- **RESTRICTED:** Information that is business data which is intended strictly for use within the City. Although most all of this information is subject to disclosure laws because of the City's status as a public entity, it still requires careful management and protection to ensure the integrity and obligations of the City's business operations and compliance requirements. It also includes data associated with internal email systems and City User account activity information.

- **CONFIDENTIAL:** Information that is very sensitive in nature and requires careful controls and protection. Unauthorized disclosure of this data could seriously and adversely impact the City or interests of individuals and organizations associated with the City. However, this information may be subject to public disclosure laws.

Below is a "Quick Reference Matrix" for minimum security measures that should be applied to systems hosting the three different data types described above. If there is any question about the categorization of data, the default classification category is "Restricted."

(See next page)

Data Classification Quick Reference Matrix for System Security Measures

DATA TYPE →	**PUBLIC**	**RESTRICTED**	**CONFIDENTIAL**
Access Control Measures	Limited to System Administration	Yes	Yes
Operating System Maintenance.	Yes	Yes	Yes
Logging	Yes	Yes	Yes
Anti-Virus Measures	Yes	Yes	Yes
Backup and Recovery	Yes	Yes	Yes
Firewalls and IDS	Optional	Recommended	Yes
Personally Identifiable Information (PII)	No	No	Yes
Credit Card or Bank transaction information	No	No	Yes
Critical Infrastructure information	No	Recommended	Yes
Encryption (During Transmission)	No	Recommended	Yes
Encryption (Storage)	No	Optional	Optional
Authentication	Limited to System Administration	Yes	Yes (2-layer Minimum)
Physical Security	Recommended	Yes	Yes

Back to Table of Contents

GUI 12A Assessing What Security Measures to Implement

All computer and data security measures are based on the functional nature and degree of criticality of the computer systems, network resources, and data involved. To assess what security measures should be implemented for a computer, the questions to ask include:

- What data is used and stored on it?
- Who uses the system?
- How do users access the system?
- What functions does it provide?
- What is the importance (criticality) of the functions?
- What is the system's connectivity to other networks and users?
- Where is the system located?
- Are there any related statutory and regulatory requirements involved?

Guidelines 12A – 12B address these questions and offer security measures and practices to evaluate for potential use in protecting computer systems' availability, confidentiality, and integrity. (See also, GUI 10A – Classification of Data)

When assessing a system's security needs, it is important to understand that all of these measures and practices offer different protections against the many risks and potential problems that exist. Taking the time to assess the security needs of a computer system is a requirement for all system owners, operators and data custodians. The only thing more important is ensuring the implementation of the necessary measures.

GUI 12B Access Control Measures

As stated in POL12, all computing systems hosted on City networks must support and comply with the following fundamental access control measures, functions and operating principles:

- All systems are required to have a technical access control mechanism of some kind that allows for authorization and allocation of system and data resources to individual users. Access mechanisms can be mandatory, transaction-based, role-based, time-based, user-based, or any other reasonable control method appropriate for the systems functions (See GUI 13G – Authentication Mechanisms for more information).

- All system access accounts for Users must be based on a unique identifier and no shared accounts are allowed except where authorized as an exception by the System Owner/Operator.

- All Users' system access will be based on the *"principle of least privilege"* and the *"principle of separation of duties"* ((See *Information Systems Security Policy*, Section 4 – DEFINITIONS)

- Computer applications that are developed for the system will be developed and integrated such that individual User accountability is maintained.

- Procedures must be in place for issuing, altering, and revoking access privileges (account ID).

Management practices adopted to support the access control mechanisms should be sensible, reasonably easy to maintain, and be auditable. They should include an electronic or paper request and approval process for all accesses established, modified, or terminated. The related System Owner/Operator and Data Custodian should maintain this process. Also, the management practices should include a regular review process of existing access accounts to make sure they are still valid.

In addition to controls that are necessary for all systems, controls are particularly important for systems and applications that host restricted or confidential data. Data access privileges should be granted and system functions defined in a manner that establishes all necessary separation of duties and helps prevent potential fraudulent actions or compromise of data. The guiding rules for this are:

- All access to critical and sensitive servers or applications for administrative purposes should require two-factor authentication.

- All access to "personally identifiable information" (PII) (See Section 4 – Definitions) requires authentication at the individual user level.

- All access to network resources where sensitive data may reside on connected system resources requires authentication at the individual user level.

- Each user will be granted access only to those hosts, services, and data for which that user has a legitimate need.

Access and privileges will be granted only for the period of time they are needed.

Back to Table of Contents

GUI 13A Operating System Maintenance

Because of the rapidly changing and vulnerable technology environment that exists today, it is very important for System/Owner Operators to properly maintain their systems. Computer systems are easily targeted and compromised through network connections. If a system is not properly secured, the odds are good that someone will compromise and exploit it.

While nothing short of physically disconnecting a system from the network will guarantee that it cannot be broken into, a number of steps should be taken to reduce the risks. The following are recommended basic maintenance practices:

Change default passwords, or disable all default accounts. Some systems come with software installed that has password protection, but with passwords that are set at the factory. These default passwords are widely available online; if this account is left running with a password which was set by the vendor, then the system is at a higher degree of risk for compromise.

Know what services should be running and which are actually running, Many systems come with services enabled that don't need to be. If a system is running an unknown service and a weakness is found in that service, the security of the system is at risk. It is important for System Owners and Operators know what is actually running on their system. If something is running that isn't needed, it should be turned off. It's better to start with everything off and turn on the services that are needed than to start with everything on and disable the services that are not needed.

Keep your operating system up-to-date. Vendors publish notices about updates and patches. Systems should be kept up-to-date with security patches as much as possible. Some operating systems come with utilities to help keep them up to date; others require more manual labor. If this task cannot be automated in the operating system, make sure there are procedures in place to regularly check for current patches.

When possible, scan your own machine for vulnerabilities… Potential intruders regularly scan networks for vulnerable machines. System Owners and Operators should use scanning tools such as Nessus to scan their systems before vulnerabilities are found by others.

GUI 13B Logging

Wise operation of a computer system and associated applications includes prudent and sensible use of logging tools. While logging can be problematic in its potential volume and usefulness of data collected, is important for System Owners and Operators to take the time to evaluate their logging needs and ensure that appropriate logging tools are implemented and maintained.

In addition to the logging itself, operational practices need to be implemented to ensure regular review of the logs for anomalies and exception events that could signal potential problems.

Logging efforts have value and are important for several reasons. In addition to supporting audits of selected system activity, security measures, and controls, a logging program also can help to resolve operational problems and contribute valuable information to security incident investigations.

The following are recommended logging practices:

- System activity associated with all “system administrator” privileged user-accounts should be logged.

- City Computer Systems that handle “restricted” or “confidential” data should securely log all significant security relevant events. Examples of security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to system or application software, and changes to user groups or accounts.

- Computer applications that support processing of “restricted” or “confidential” data should log the following key user activity information:
    1) User session activity including user-Ids, log-in date/time, log-out date/time and applications invoked;
    2) Changes to key application system files;
    3) Additions and changes to the privileges of users; and
    4) System start-ups and shut-downs.

It is important to establish appropriate retention practices for various logs. It is recommended that logs containing security relevant events be retained for at least one month or longer if feasible. These logs are important for system effort correction, forensic auditing, security breach investigations, and related efforts. It is important that stored logs must be secured such that they cannot be modified and only authorized persons have access to them.

GUI 13C Antivirus Measures

It is well known that one of the major threats to computer systems and data is exposure to malicious code. Viruses, worms, Trojan horse programs, and other such threats are difficult to defend against and require a systematic approach to mitigate the potential harm.

System Owners and Operators should install and maintain high quality anti-virus systems on their file servers and ensure that all system-associated desktop computers have the same kind of protection installed and maintained. System Owners and Operators should be vigilant about loading all updates to the anti-virus software as they become available.

In addition to anti-virus software, it is important for System Owner and Operators to establish infection prevention and damage mitigation procedures that include:

- Scans of all diskettes and other portable storage media before they are loaded into the system;
- Scans of all files downloaded from the Internet;
- Rules against the use of any software that is not obtained legally through reliable sources; and
- Response procedures for dealing with infection or attack by malicious software

GUI 13D Backup, Recovery and Data Retention

In order to protect their computer systems and data, System Owners and Operators must implement regular backup procedures. Regular backups of all critical system software, applications, and data are necessary for both recovery and compliance purposes. The frequency of these backup processes also should be sufficient to support the documented contingency plans.

When choosing the location for the storage of backup media, it is important to make certain that it is protected from access, change, or unwarranted destruction. The level of security associated with the backups should be the same as that for the disk copy. Additionally, backup media should be stored at a separate “off site” location that is unlikely to be affected by any disasters befalling the primary copy of the data.

Data retention is a separate issue from backup. Backups rarely, if ever, should be counted upon as the means for records retention management. City Data

Custodians, System Owner and Operators, and Users are obligated to understand the nature of the data they generate, use, or store and to ensure that they are managing that data in full compliance with all applicable laws and City records management policies (for Records Retention information see Appendix B- Relate Documents).

GUI 13E Firewalls and Intrusion Detection Security

At the City, effective host-based security measures are wise for System Owner and Operators to deploy and maintain. System Owners and Operators must consider carefully how they manage their network connectivity and what filtering tools and rules work best for their computing needs.

The City has deployed firewall systems on the City's network perimeter. However, because of the complex computing environment that exists at the City and the wide-range of computing services required, the City departments should consider a layered defense that includes protection at the Internet, demilitarized zone (DMZ), internal network segmentation, and host-based systems.

The following are recommended firewall and intrusion detection practices:

- Firewalls should be used to secure Internet connections;
- Firewalls should be considered for any connection to other networks;
- A boundary firewall should be used at the Internet connection to create an external DMZ;
    - Servers accessible by the public should be placed on the DMZ so they can be accessible as needed and still have some protections from the firewall;
    - Internal users should be protected from the external sources as well as the DMZ by the firewall;
- A firewall standard document should be created and maintained that details firewall environment functions, file characteristics, network applications matrix, and traffic handling policy;
- Firewall administration should be assigned to only qualified and dedicated technical staff;
- Critical networks or hosts can be protected through the use of internal firewalls or firebox systems;
    - Departments should carefully evaluate this option as a potential extra layer of security;
- Remote locations should use personal firewalls and firewall appliances to secure their connections;
- Network intrusion detection systems (IDS) should be used at external connections as additional safeguards against attacks;

- Critical networks can be protected through the use of internal network-based IDS or host-based IDS;
    - Departments should carefully evaluate this option as a potential extra layer of security;
- IDS administration should be assigned to only qualified and dedicated technical staff;
- Logs from the various firewalls and IDS systems that are installed and maintained should be aggregated to a dedicated server to the extent possible;
    - This provides the ability to correlate suspicious activity as well as one-stop monitoring for security event information
    - This aggregate logging system needs to take into consideration the sensitivity needs of the systems involved and provide appropriate access controls;
- Automated alarms that initiate alerts to pager, email, and/or voice message systems should be considered; and
- Appropriate incident response procedures and practices should be developed and implemented to support firewall and IDS alerts.

Another option to consider for protecting the Users' desktop systems is installing "personal firewalls" (firewall rules which run on the client itself). There are several types of these firewalls currently available and properly implemented they can be very useful as part of a larger security strategy for a subnet.

Some personal firewall products also include Intrusion Detection System (IDS) capabilities that might be useful. IDSs are often closely tied with firewall implementations.

Besides host based IDSs, there are also some network-based systems. Again, it is important that System Owners and Operators evaluate their specific security requirements and understand if these systems offer any value to security objectives.

GUI 13F Encryption

Implemented and used wisely, encryption can support a variety of security objectives for System Owners and Operators including authentication, integrity, privacy, and non-repudiation objectives. However, there are some difficult challenges for System Owners and Operators to effectively deploy encryption tools and doing so will likely require careful review and consideration.

A few approaches to encryption are being used and explored at the City. However, there are some difficult and substantial barriers to widespread deployment. In addition, to the implementation issues with standards and

methods, encryption tools themselves can be abused by users potentially leading to the loss of access to data, corruption of data, and other problems. System Owners and Operators should not deploy encryption tools without implementing strict use and management practices. Most importantly, System Owners and Operators should never allow unauthorized encryption tools to be used on their systems.

GUI 13G Authentication Mechanisms

A key security measure that System Owners and Operators need to implement is a means to authenticate system users. There must be a systematic and reliable method for establishing proof of identity. Authentication mechanisms are closely woven into system access controls. For System Owners and Operators it is important to remember the difference between authentication and authorization mechanisms. One identifies a user and the other defines what the identified user can access. Both sets of mechanisms need to be carefully implemented and maintained.

There are essentially only three "ways" a user can prove their identity:

- With something they **know**.
  (Technology translation: passwords, personal identification numbers, pass phrases, secrets)
- With something they **have**.
  (Technology translation: token, smart card, certificate, private key)
- With something they **are**.
  (Technology translation: biometrics, activity signatures)

The criticality of the computer systems and the sensitivity of the data determine the kind of authentication process that should be implemented. Some circumstances require the use of a two-layer approach to authenticate a user to a system. This layered approach increases the difficulty for an unauthorized person to fool the system's authentication process.

System Owners and Operators and data custodians must evaluate their system's authentication requirements and implement the appropriate measures. This evaluation process should not minimize the reality of the situation—existing technologies are vulnerable and can be spoofed.

The most basic protections come from establishing systems and processes that assure that good passwords are created, maintained, and correctly transmitted. Software is available to force the choice of good passwords and check periodically for weak ones. Passwords should be changed regularly. Only protocols that encrypt passwords should be used to transmit them over the network.

GUI 13H Use of Secure Protocols

System Owners and Operators must be aware of sensitive data on their systems and use secure protocols such as SSL, SSH or K5 to protect them in transit or for access of services that require authentication.

GUI 13I Use of Security Warning Banner

System Owners and Operators should use a banner similar to the one below:

,

WARNING

This is a proprietary system of the City of Seattle and is for use by authorized individuals only.

Use of this system or any other computer system of the City of Seattle constitutes an express consent to monitoring at all times. If monitoring of any City system for either administrative, enforcement, or management purposes reveals possible violations of criminal statues, all relevant information may be provided to law enforcement officials. Anyone using this or any other City computer system or related information without proper authorization will be subject to possible internal disciplinary actions, civil and/or criminal prosecution. By proceeding beyond this screen you are acknowledging that you understand and accept the content of this notice.

Back to Table of Contents

GUI 13J Multifunction Device Configuration Guidelines

Devices that contain a modem or other external connection and contain an operating system present a specific risk to the City's system due to the connection between untrusted phone systems, the City's network, and the vulnerability of the operating system.
To mitigate those risks, it is imperative that these types of devices (e.g. multifunction printer/fax machines) be installed and configured carefully.
The following are recommended configuration guidelines for these types of devices:

- All administrative account passwords (i.e. ADMIN, MSHELL, LOCAL) must be reset;
- Any services not required must be turned off - these include:
  - SMTP;
  - FTP;
  - Telnet;
  - Bluetooth;
  - and 802.11 (if equipped);
- TCP/IP must be set as the only active protocol;
- Enable restriction of IP's able to access device and restrict them to the local segment;
- Disable the ability for the device to store scanned documents locally;
- Register the device per City Policy to SMTP(2) gateway, registering Device Name and IP;
- Reference the device manufacturer's security recommendations and apply them as appropriate;
- Document all install processes and security settings and keep this document on file in your IT management offices for audit reference.

Back to Table of Contents

GUI 14 Physical Security Guidelines

To prevent portable electronic devices such as laptops, personal digital assistants (PDAs), cell phones, or USB drives from being stolen or misused requires keeping them physically secure.

Some examples and best practices would include:

- Never leaving a portable electronic device unattended when you take them outside the office;
- Never leaving them in your hotel room or car (even in a locked trunk);
- Never leaving them in checked luggage
- Always locking laptops with a cable lock when they are on your desk at work, or if you have to leave them in a hotel room, and
- Storing them in a locked cabinet at work or at home when you are away.

Physical access control measures for City property should include:

- Access control badges that are worn in plain site and are required for entry into any area where City assets are located;
- Monitored video cameras in strategic locations to record activities;
- Guards in all City buildings to monitor physical security, and
- Monitoring of visitors including requiring registration, visitor badges and escorts whenever they are in areas where City assets are located.

Back to Table of Contents

GUI 15 Suggested Components of User Termination Process

All City departments should establish and maintain all necessary processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is separated. These processes and procedures should include the following:

a. The separated employee's immediate management will be responsible for notifying all System Owner/Operators, or their designated system administrator handling the computer or communications accounts, to close all related accounts and remove all access capabilities related to the terminated employee.

b. Separated employees may not retain, give away or remove from City premises any City proprietary information (electronic or hardcopy) other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other City proprietary information in the custody of the departing employee must be turned over to the employee's immediate supervisor at the time of departure.

c. At the time of separation, all City property must be returned. This includes portable computers, printers, modems, software, cellular telephones, digital pagers, PDA's, documentation, building keys, lock combinations, encryption keys, and magnetic access cards.

Back to Table of Contents

GUI 17A Prohibited Uses of City-owned Digital Equipment

City equipment may not be used for any of the following purposes as defined by City policy, ethics rules and City and State laws (this is not necessarily an all inclusive list – others may apply and the user is charged with using discretion):

- conducting private business;
- political campaigning;
- announcing union membership meetings or conducting other exclusively union business;
- making unauthorized general message distributions to all users ("everyone");
- sharing or storing unlicensed software or audio/video files;
- or any other illegal usage.

GUI 17B Installation of Hardware/Software

Only software or hardware that meets the City's defined standards (see Appendix B – Related Documents) will be installed unless an exception has been documented in writing.

This includes but is not limited to applications specifically designed to communicate electronically. Electronic communication technology poses a particular security risk due to the two-way nature of these applications.

Examples of electronic communication technology requiring a written exception include instant messaging (IM), voice over IP (VoIP), and Internet Relay Chat (IRC). To obtain an exception see PRO 23.

GUI 17C Use of Bandwidth Intensive Application/Features

Use of video, audio, image storage, etc. can put a strain on the available resources of the City's networks and bandwidth. The Office of Information Security reserves the right to require a review of any usage that is discovered to have strained the City's resources.

Users should work with their IT management to establish the resource and bandwidth requirements of any new applications or systems. In collaboration with departmental IT management all new applications or projects should be assessed for any possible negative effects due to resource strain. If it is suspected that strain could be caused by the proposed application or system, it should be reviewed and approved in writing by the CTO as required in POL17, paragraph 4.

GUI 17D Guidance on De-Minimus Use of City Digital Equipment

To the extent permitted by your department's policies, you may use City owned digital equipment, access to the Internet, and other applications including e-mail and other authorized electronic communications such as Instant Messaging, to announce or distribute notice of departmental or personal events of interest to your co-workers. However, all messages announcing or promoting an event such as a training opportunity, charitable fund raising campaign or other presentation must be approved by a designated management representative before they are disseminated universally across any e-mail facility.

You may also use these resources to schedule personal appointments and for other reasonable personal purposes as long as such use is incidental and does not interfere with your workload, as determined by your supervisor.

Back to Table of Contents

GUI 18A Individual Screening of E-Mail

Users are allowed under this policy to screen unwanted e-mail from, or to automate filing of, their individual e-mail accounts using methods including:

- the employment of automated e-mail screening rules;
- the use of mailbox proxies (for example, the granting of permissions to another user or users to objects in a mailbox);
- or other manual or automated screening techniques that are consistent with all other citywide and department standards

GUI 18B Guidance for Sending Public Electronic Communications

Care must be taken when sending electronic communications from the City of Seattle to the public. It is the responsibility of every user to understand and comply with the City's published Privacy Policy and this Information Security policy when doing so (See Appendix B – Related Documents). To ensure all such communications are consistent with those policies requires:

- the intended recipient specifically request ("opt-in") to receive the communication from the City;
- the proper protection of personally identifiable information- such as a person's e-mail address;
    - For instance senders of public e-mail broadcasts must take steps to conceal the intended recipients e-mail address from others receiving the broadcast (this can most easily be accomplished through the use of the blind carbon copy (BCC) feature).
    - Users of other electronic communications, such as Instant Messaging should never reveal their buddy lists or communicate with unknown users.

GUI 18C Guidelines for General Distribution Message Within or Between City Departments

It is sometimes necessary to inform a department of news of interest or importance to all users. When this is the case, care must be taken that any such messages are approved by the departmental management.

All general broadcast messages to be sent to all users of a department by another department must be cleared by the receiving department

The message must be forwarded first to the Departmental e-mail Administrator of that department, so that it can be reviewed and approved and properly staged and transmitted so as to not disrupt normal e-mail operations.

Back to Table of Contents

GUI 21a Guidelines to Secure Remote and Ad Hoc Devices

1. Departments authorizing remote and ad hoc connections should establish appropriate connectivity management processes that will, at a minimum, audit and monitor for anti-virus signatures and required operating system patches.

2. Departments authorizing remote and ad hoc connections should scan computing devices for the existence of malicious code and programs

3. Ad hoc users who are connected the Network should not be connected to any other network at the same time

4. Dual homing (see Section 4 – Definitions) is an unsafe connectivity practice and is allowed only on an exception basis

SECTION 4 – DEFINITIONS

Jump to: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

The following terms are found in this policy document:

802.11x: A generic term used to describe any of the currently deployed wireless standards (currently this includes 802.11a, 802.11b, 802.11g, and 802.11n)

Acceptable Use Agreement: An agreement outlining policies, guidelines, responsibilities for Authorized Users granted remote access to the Network. The Agreement must be signed and returned to the granting department.

Access Control: Physical, procedural and/or electronic mechanism which ensures that only those who are authorized to view, update and/or delete data can access that data.

Ad Hoc Connectivity: Plugging an ad hoc device directly into the Network or another City owned workstation while on City premises for the purposes of accessing City applications, the Internet and/or other City data resources.
Top of Definitions Section

Ad Hoc Device: City or non-City owned devices that have not been connected to the Network within the preceding month or a specific period of time designated by departmental policy. Because they have not been connected, they are considered “untrusted” and assumed to be non-compliant with current patching levels.

Ad Hoc User: Employees, contractors, business partners, etc., who are not Authorized Users, but have a need, on a temporary basis, to connect to the City network to conduct City business.

Applications Software: Applications software comprises programs designed for an end user, such as word processors, database systems, and spreadsheet programs.

Authentication: A systematic method for establishing proof of identity.

Authorization: The process of giving someone permission to do or have something; a system administrator defines for the system which users are allowed access to the system and what privileges are assigned.

Authorized User: A City permanent or temporary employee who has been granted the use of a wireless enabled computing device in order to conduct City business.

Availability: The assurance that a computer system is accessible by authorized users whenever needed or as pre-defined.

Breach: An incident that compromises the confidentiality, integrity or accessibility of data on any City owned system. A “reportable” security breach is defined by Washington State Law as noted in POL 11 in this handbook.
Top of Definitions Section

Cable Modem: Cable companies such as Comcast provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Cyber Incident Response Plan: The Cyber Incident Response Plan outlines the responsibilities and procedures for responding to any event that significantly impacts or threatens the City's information systems.

Cyber Incident Response Team (CIRT): A team of departmental IT staff and managers from all City departments, who have been selected to work with the command staff on any formal cyber incident.

Cyber Incident Response Triage Team: A small select group of Information Security staff representing a cross section of different departments whose task is to establish the severity of any threatening event and decide whether to initiate the Cyber Incident Response Plan.

CISO: Chief Information Security Officer

Common Criteria for Information Security Evaluation: A comprehensive specification (aligned with the ISO IS 15408) that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.
Top of Definitions Section

Computing Device: A device such as a desktop, laptop, handheld, or notebook computer, Personal Digital Assistant (PDA), or a server.

Confidentiality: An attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial.

Connectivity Management: Controlled access to Network resources by allowing only computing devices that fully comply with established criteria; that is, current operating system patch levels, up-to-date virus signatures and the absence of specific worm, virus, or Trojan malware. Ad hoc devices will be denied access or will be quarantined in a holding queue. Connectivity management can be achieved through combinations of process, procedures, and hardware/software.

Contracted Vendor: A vendor who, through agreement and contract with the City, will provide technical support on City applications or software via a remote connection on the Network.

Cookie: A small text file that is sent to a user's computer by the server that the user is visiting. This file can record preferences and other data about the user's visit to a particular site. Cookies often are used for long-term data collection. Short-term cookies might be used for things like authentication in "single sign-on" services.

Cost-effective: To deliver desired results in beneficial financial terms.
Top of Definitions Section

Critical Patches: In this document, the term is used to prioritize patches that are determined, by City of Seattle technical staff. Generally, this rating should correspond to patch ratings offered by vendors; however, in some cases, this may not always hold true specific to the City's technical environment.

Data Custodians: Individuals who have been officially designated as being accountable for protecting the confidentiality of specific data that is transmitted, used, and stored on a system or systems within a department or administrative agency of the City.

Data Storage Device: A device that may or may not have intelligence that is connected to the Network via a network port, or by insertion into a computing device port that is connected to the Network. These devices are generally used to store data.

Decryption: The process of turning unreadable cipher text into readable text.

Device: Any piece of hardware that uses system or application software to logically connect to an IP address within the Network. Examples are laptop, desktop, or notebook computers, PDA's, digital cameras, or servers.
Top of Definitions Section

Dial-up: A method of communicating via telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device.

Examples include but are not limited to:

1. Connecting a server to two different networks using two network interface cards (NIC).
2. Connecting a computer to a City provided DSL, ISDN, or cable modem AND concurrently connecting to a public ISP, a bulletin board, or a family member's network via modem or publicly provisioned broadband.
3. Configuring an ISDN router to dial into City and an ISP, depending on packet destination.
4. Connecting a computing device to the Network and concurrently using a modem to connect to another network (whether wired or wireless).

Due Care: Due care is the collective steps that an organization must take to properly protect its networks, computer systems and the data that resides on them.

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 1.5 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Top of Definitions Section

DMZ - De-Militarized Zone: A separate part of an organization's network which is shielded and 'cut off ' from the main corporate network and its systems. The DMZ contains technical equipment to prevent access from external parties (say on the Internet) from gaining access to your main systems.. A DMZ is not a single security component; it signifies a capability. Within the DMZ will be found firewalls, choke and access routers, front-end and back-end servers. Essentially, the DMZ provides multi-layer filtering and screening to completely block off access to the corporate network and data. And, even where a legitimate and authorized external query requests corporate data, no direct connection will be permitted from the external client, only a back-end server will issue the request (which may require additional authentication) from the internal corporate network. However, the extent to which you permit corporate data to be accessible from and by external sources will depend upon the value of the Business Assets which could be placed at (additional) risk by allowing access to (even) pre-specified data types

Encryption: The process of turning readable text into unreadable cipher text.

Firewalls: Are policy-based filtering systems (composed of both hardware and software) which control and restrict the flow of data between networked computer systems. Firewalls establish a physical or logical perimeter where selected types of network traffic may be blocked. Blocking policies are typically based on computer IP addresses or protocol type of application (e.g. web access or file transfer). Types of firewalls relevant to this policy include:

- Dedicated firewalls protecting network gateways
- Proxy servers
- Routers acting as firewalls

Top of Definitions Section

Forensics (computer): The discipline of dissecting computer storage media, log analysis, and general systems and data examination to find evidence of computer crime or other violations of law or policy.

Frame Relay: A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame relay has a flat-rate billing charge instead of a per time usage. Frame relay connects via the telephone company's network.

Holding Queue: A logical network location for ad hoc devices that contains compliance remediation services. This holding queue will be separated from the Network such that non-compliant devices cannot affect or infect other computing devices or Network resources. This queue may be a single disconnected PC, that ad hoc devices can be connected to, or a VLAN with server remediation services.

Host-based Intrusion Detection System HIDS): (See IDS) A Host IDS (HIDS) is set up to detect illegal actions within the host computer. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Top of Definitions Section

Incident Response: The ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source at anytime.

Information Technology Managers: Individuals within the City who are accountable for the operational decisions about the use and management of a computing system. (See also, system owners).

Integrity: The condition of data or a system, which is that it remains intact, unaltered, and hence reliable.

Internet: The Internet is made up of computers in more than 100 countries covering commercial, academic and government endeavors. Originally developed for the US military, the Internet has become widely used for academic and commercial research. Users have access to unpublished data and journals on a huge variety of subjects. Today, the Internet has become commercialized into a worldwide information highway, providing access to information on every subject known to humankind.

Intrusion Detection System (IDS): A security management system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attack from outside the organization) and misuse (attacks from within the organization).
Top of Definitions Section

ISDN: Integrated Services Digital Network. Provides for point to point data transmission at 128K bps. ISDN users must connect to a host, which is also capable of ISDN connection using an adaptor. The reliability of ISDN is not questioned, however, it is relatively expensive and is being eclipsed by the recent growth in broadband Digital Subscriber Line (DSL) technology.

ISP: An Internet Service Provider - commonly referred to as an 'ISP', is a company which provides individuals and organizations access to the Internet, plus a range of standard services such as e-mail and the hosting (running) of personal and corporate Web sites. The larger ISPs will offer a range of access methods including telephone, leased line, ISDN or the newer DSL (ADSL) circuits and will be connected to 'backbone' high speed digital circuits which form the Internet itself. ISPs usually charge a tariff for their services although income can be derived from various sources of advertising and portal activities. Occasionally an ISP are referred to as IAP - an Internet Access provider

LAN: A home or office network operated within one location. This may comprise one or more adjacent buildings, but a local network will normally be connected by fixed wires. For purposes of this policy, a router that connects multiple computing devices at home is considered a LAN.
Remote Access: Any access to the City's network through a non-city controlled network, device, or medium.
Top of Definitions Section

Network-based Intrusion Detection System (NIDS): (See IDS & HIDS) A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host computer. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Non-repudiation: A mutually agreed process, secured evidence, or other method of operation which provides for proof of receipt or protection from denial of an electronic transaction or other activity.

Off Site: A location separate and distinct from the area in which something, such as a computer, is located. Frequently referred to when considering backup storage.

OIS: Office of Information Security. Consisting of the Chief Information Security Officer, Deputy Chief Information Security Officer and any assigned staff.

Ownership: The term that signifies decision-making authority and accountability for a given span of control.

Perimeter Security: The ability to protect the outer limits of a network, or a physical area, or both.
Top of Definitions Section

Personally Identifiable Information: specific data, elements of non-specific aggregate data, or other information which is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a person as an individual and make personal information about them known.

Principle of Least Privilege: An operations principle that requires access privileges for any user to be limited to only what they need to have (nothing in addition) to be able to complete their assigned duties or functions.

Principle of Separation of Duties: An operations principle that requires that whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.

Privacy: An individual right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property.

Privacy Statement: Sometimes referred to as a privacy policy, a privacy statement is posted on an organization's Web site to notify visitors of the types of information being collected and what will be done with the information.
Top of Definitions Section

Proxy Server: A proxy server is a computer network service which allows workstation web browsing clients to make indirect web (or other network) connections to other web services or pages. A client connects to the proxy server, and then requests a connection, file, or other resource available on a different server. This can be legitimately used to increase security by giving administrators a way to control Internet access and network connections. However, it can also be used to bypass legitimate controls by re-directing service or web browsing requests around enterprise servers.

Remote Access: Any access to the City's network through a non-city controlled network, device, or medium.

Risk Management: A comprehensive methodology that strives to balance risks against benefits in a pre-defined environment.

Security: An attribute of information systems which includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the privacy of individuals.

Security Guidelines: Recommended actions and/or industry best practices that should be used as a compass by users, IT staff, and others regarding security practices. Guidelines are not considered compulsory but instead treated as recommendations.
Top of Definitions Section

Security Policy: Set of organizational rules and specified or implied practices that regulate how an organization manages, protects and uses its information systems assets and data. These are rigid and must be complied with and any exceptions to them documented, reviewed and approved. A Security Policy works as a blueprint for an organizations security program.

Security Standards: Rules indicating how and what kind of software, hardware, databases and business practices should be implemented, used and maintained to meet security and operational objectives. Standards are normally considered compulsory like policy statements.

Service Pack: A service pack is an update to an operating system or application that includes coding and feature enhancements or revisions. It can also address security vulnerabilities as part of its package of revisions.

Split Tunnel: This term has meaning only for VPN tunnels. It is the definition of how network traffic is handled by a remote end of a VPN tunnel. If using a split tunnel, then traffic bound for the City's network uses the VPN tunnel and traffic bound for anywhere else, is not sent to the city, but rather is handled as normal by the ISP. If not using split tunnel, then when the tunnel is up, any traffic from the remote computing device is sent through the tunnel and handled by the City network. The choice of using a split tunnel or not is NOT configurable by the VPN client.
Top of Definitions Section

Spoofing: The interception, alteration, and retransmission of data (in an attempt) to fool the recipient.

SSL VPN: A secure socket layer (SSL) VPN tunneling method that employs SSL encryption protocol.

System: A network, computer, software package, or other entity for which there can be security concerns.

System Administrators: Individuals who support the operations and integrity of computing systems and their use. These activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. In an inter-networked computing environment, managing the computer network often is their responsibility.

System Management: The activities performed by systems administrators.

System Owners: Individuals within the City who are accountable for the budget, management, and use of one or more electronic information systems or electronic applications that are associated with the City.
Top of Definitions Section

System Operators: Individuals within the City who are accountable for the operational decisions about the use and management of a computing system. (See also, system owners).

Systems Software: Systems software refers to the operating system and all utility programs that control computer resources. For purposes of this policy, it also covers firmware, or "embedded" software, such as the software that runs on a Dell remote access card, which has a web server embedded within the card itself.

Untrusted Image: A file containing an operating system, applications, services etc. that is used to custom configure a computing device specific to the needs of a particular organization. An untrusted image file is one that has not been updated to current patching and virus signature levels and is therefore untrusted and should not be used.

Users: Any individual that has been granted privileges and access to City computing and network services, applications, resources, and information.

VLAN: Short for virtual LAN, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a Local Area Network (LAN). VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration

VPN: A Virtual Private Network (VPN) tunnel is a method for accessing a remote network via "tunneling" through the Internet.
Top of Definitions Section

Wired: Generally refers to the physical cabling in a network. “Over the wire” means transmitting the signal onto the physical medium. Increasingly, the wire is not longer metal, but glass. In this policy, a “wired” connection is one that is connected directly to the City’s backbone network without having passed through any wireless or Internet connection.

Wireless: Radio transmission via the airwaves. Various communications techniques are used to provide wireless transmission, including infrared line of sight, cellular, microwave, Bluetooth, satellite, packet radio and spread spectrum. This policy covers the use of any wireless technologies used or contemplated for use in City communications or IT systems.

Top of Definitions Section

Back to Table of Contents

SECTION 5 – DOCUMENT CONTROL

***Owning Organization**:* City of Seattle DoIT Office of Information Security (OIS)
Update Cycle: To be reviewed annually for possible changes or considered for change at any time if requested.
Record of Versions:

Version	Status/Comments	Date
	Updates and minor changes, for public disclosure – by Robert Cazares	04/07/2011
Re-write v4.3	Clarifications in VPN procedures & VPN Acceptable Use Sample	8/1/07
Re-write v4.2	Clarifications in Remote Ad Hoc procedures section by DRM	6/19/07
Re-write v4.1	Clarifications and grammatical edits by DRM	6/1/07
Re-write v.4	Rewritten for policy standardization by David Matthews (no substantive changes)	5/24/07
Re-write v3.1e	Minor re-writes for clarification – sign off by CTO	4/25/07
Final v 3.1d	Reviewed by OIS, ITSB and accepted by CTO	1/2/2007
Draft v 3.1c	Tech Council and ITSB changes incorporated	12/20/06
Draft v 3.1	ITSB changes incorporated by David Matthews	11/17/06
Draft v 2.1	ITSB changes incorporated by David Matthews	10/15/06
Draft v. 1.1	ITSB changes incorporated by David Matthews	9/15/06
	Review by ITSB	9/7/06
Draft V 1.0	Written by David Matthews (replacing ISSP v.2 adopted October 2003)	8/25/06

Back to Table of Contents

APPENDIX A – REGULATORY AND COMPLIANCE REQUIREMENTS

The information contained in Appendix A is for the reader's convenience only. It should be understood that the City makes no representation as to the completeness, accuracy, or currency of the materials.

City, State and Federal statues and regulations that directly or indirectly affect City of Seattle's information systems security program include:

Seattle Municipal Code

- SMC 14.04 – relating to fair employment practices
- SMC 14.12 – relating to the collection of criminal information

Revised Code of Washington (RCW)

- RCW 40.14 - relating to records management, retention and destruction.
- RCW 42.17.020 – relating to public records "writing" inclusive of graphics and computer records.
- RCW 42.17.310 – relating to private and vital public records that are exempt from disclosure.
- RCW 5.60.060 – relating to communications made to a public officer in official confidence, when the public interest would suffer by disclosure.
- RCW 42.52.050 – relating to confidential information records improperly concealed.
- RCW 42.52.260 – relating to documents and indexes to be made public.
- Chapter 70.02 RCW - Uniform Health Care Information Act
- RCW 71.05.390 - 420 – relating to mental health records.
- RCW 71.34.200 – relating to mental health care record of juveniles
- RCW 70.24.105 – relating to HIV/STD information
- RCW 9.73 – Privacy Act
- RCW 19.190.020 - Unsolicited Electronic Mail Act
- RCW 9A.48.100 – Malicious Mischief
- RCW 9A.52.110, 120, 130 – Computer Trespass

Washington Administrative Code (WAC)

- WAC 478-250 – relating to governance for indexing of public records.
- WAC 478- 276 – relating to governance for access to public records.
- WAC 292.130 – relating to protection and management of public records.

United States Code (U.S.C.)

- (5 U.S.C. § 552a) Privacy Act – relating to the collection, notification, disclosure, and handling requirements of personal data.
- (18 U.S.C. § 2701, et seq.) Electronic Communications Privacy Act – relating to prohibitions for persons tampering with computers or accessing certain computerized records, without authorization. The act also prohibits providers of electronic communications services from disclosing the contents of stored communications.
- (Pub, Law No. 104-191 §§ 262,264: C.F.R. §§ 160-164) Health Insurance Portability and Accountability Act – relating to the security and privacy of individually identifiable health information that is maintained or transmitted by a covered entity. Also it requires these

covered entities to apply many of its provisions to their business associates, researchers, employers and others.

- (42 U.S.C. § 242m) – relating to prohibitions of disclosure of data collected by the National Centers for Heath Services Research and for Health Statistics that would identify an individual in any way.
- (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3) Drug and Alcoholism Abuse Confidentiality Statutes – relating to prohibition of disclosure of information collected for federally funded research and treatment of drug abuse and alcoholism.
- (5 U.S.C. § 552) Freedom of Information Act [FOIA] – relating to provisions for access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information.
- (39 U.S.C. § 3623) Mail Privacy Statute – relating to prohibitions of opening mail without a search warrant or the addressee's consent.
- (29 U.S.C. § 1025, et seq.) Employee Retirement Income Security Act - relating to employer requirements to provide employees access to information about their accrued retirement benefits.
- (42 U.S.C. § 2000e, et seq.) Equal Employment Opportunity Act – relating to restrictions on the collection and use of information that would result in employment discrimination on the basis of race, sex, religion, national origin and a variety of other characteristics.
- (18 U.S.C. § 1029) Fraud and Related Activity in Connection with Access Devices – relating to prohibitions and penalties associated with unauthorized possession and fraudulent use of access tokens, passwords, etc.
- (18 U.S.C. § 1030) Fraud and Related Activity in Connection with Computers –related to prohibitions of unauthorized access and use of electronic systems.
- (18 U.S.C. § 1362) Communication Lines, Stations, or Systems – relating to prohibitions of malicious or willful destruction or intent to destroy or disrupt communications systems within the U.S.
- (18 U.S.C. §§ 2510, et seq.; 47 U.S.C. § 605) Wiretap Statutes – relating to prohibitions of the use of eavesdropping technology and the interception of electronic mail, radio communications, data transmission and telephone calls without consent.
- (18 U.S.C. § 2703) Requirements for Government Access –relating to rules for government agencies for obtaining disclosure of an electronic communication from a provider of such services.
- (47 U.S.C. § 1001) Communications Assistance for Law Enforcement – relating to preserving law enforcements ability to engage in lawful electronic surveillance in the face of new technological developments.
- (15 U.S.C. §§ 6501 et seq. 16 C.F.R. § 312) Children's Online Privacy Protection Act of 1998 – relating to requirements that a web site directed at children under 13 years of age to obtain "verifiable parental consent" before collection personal information from children.
- (H.R. 3162) "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001" – relating to a variety of special laws specific to countering terrorist acts including expanded investigative options for law enforcement.
- 28 CFR Part 20, Section 20.33 and elsewhere –relating to restrictions on criminal history records remaining in control of criminal justice agencies.
- (17 U.S.C § 101, et. Seq) – relating to the Copyright Act

Note: Also, to be included in this section of the listing are statutes and promulgated regulations related to NERC, FERC, WECC, GISRA and other energy sector related rules that could affect technology security policy.

Other primary authorities to be considered for conforming to best practices and strategic planning include:

- OMB Circular NO. A-130. This Circular provides uniform information resources management policies as required by many Federal Executive Orders and Acts including: 44 U.S.C. 35 – Paperwork Reduction Act of 1980, 5 U.S.C. 552a – The Privacy Act, 40 U.S.C. 759 – The Computer Security Act of 1987.
- NCQA Advisory Information System Standards (based on work presented in HEDIS Volume 4: *A Roadmap for Information Systems*
- NAIC Health Information Privacy Model Act (1998)

Additional Information Sources Regarding Policy formulation:

- National Institute of Standards and Technology (NIST) Engineering Principles for IT Security.
- NIST Special Publications 800-12, 800-14, 800-16
- US DHHS OIG Audit Practices
- National Research Council report For the Record: *Protecting Electronic Health Information* (1997)
- Common Criteria …specifically:

- *The Common Criteria for Information Technology Security Evaluation* (CC), version 2.1/aligned with ISO IS 15408 (last updated: 19 September 2000)
- *Guide for Production of Protection Profiles and Security*, Preliminary Draft Technical Report (PDTR) (last updated: 01 January 2000)
- *CSPP – Guidance for COTS Security Protection Profiles*, version 1.0 NISTIR 6462 (final document: 01 January 2000)
- *CSPP-OS Operating System Protection Profile*, draft version 0.3, (last updated: 01 April 2000)
- *Role-Based Access Control (RBAC) Protection Profile,* final version 1.0
- *Federal Government Firewall Protection Profiles*, draft version based on CC version 2.0
- *SCPP – Smart Card Security Users Group Protection Profile*, version 2.0 (last updated: 01 June 2000

Note: *All Common Criteria are established and maintained by processes and oversight of:*

The Communications Security Establishment (CSE), Canada
The Central Service for Information Systems Security (CSISS), France
The German Information Security Agency (GISA), Germany
The National Communications Security Agency (NCSA), Netherlands
The Communications–Electronics Security Group (CESG), UK
The National Institute of Standards and Technology (NIST), United States
The National Security Agency (NSA), United States

(Years ago, these organizations recognized a growing need for a common set of security criteria. This collaborative effort produced a set of standards for building and evaluating security standards, environments, and systems. These Common Criteria have now become an important authority and are being used to support legislated and regulatory standards at the national and international level. The City can anticipate that all efforts to comply with the Common Criteria will be beneficial on several technical and business levels.)

Back to Table of Contents

APPENDIX B – RELATED DOCUMENTS

System Administrator Code of Ethics

Digital Investigation Procedures:

Desktop and Laptop Standards (including configuration):

Records Retention:

Personnel Rule 1.1 – Workplace Harassment:

Online Privacy Policy
http://www.cityofseattle.net/pan/privacypol.htm

Web Application Layered Defense (WALD) Procedures document:

Modification Changes Checklist for Applications moving to WALD:

Production Readiness Assessment :

Back to Table of Contents